# Public Verifiability as a Constitutional Requirement: A Legal Thesis on the Brazilian Electronic Voting System

Abstract

This paper advances the legal thesis that the Brazilian regulatory framework governing the electronic voting system is incompatible with the Federal Constitution and the Brazilian Access to Information Act (Law No. 12,527/2011) insofar as it prevents the eventual public disclosure of the complete voting software, its deterministic build environment, and all artifacts necessary for independent verification of the binaries deployed in elections. This argument does not depend on allegations of fraud. Rather, it is grounded in the constitutional principles of publicity, transparency, democratic accountability, and public oversight.

1. Democracy Requires Verifiability, Not Mere Institutional Trust

The legitimacy of democratic elections ultimately rests on the ability of citizens to verify that votes are counted exactly as cast. While institutional trust is important, constitutional democracies should strive to replace trust wherever technically feasible with objective, independent verification.

In modern computer science, critical software systems increasingly rely on reproducible (deterministic) builds, cryptographic verification, and public auditing. These practices minimize the need for blind trust by allowing independent experts to verify that the executable software exactly corresponds to its publicly available source code.

Because election software constitutes the core mechanism through which political sovereignty is exercised, it should be subject to the highest achievable standard of transparency.

2. Constitutional Foundations

This thesis is based on several provisions of the Brazilian Federal Constitution.

Article 37 establishes publicity as one of the governing principles of Public Administration. Publicity is not merely procedural transparency; it is a constitutional mechanism enabling public oversight and democratic accountability.

Article 5, XXXIII guarantees the right of every individual to receive information of personal or collective interest held by public authorities, subject only to legally defined exceptions involving the security of society or the State.

Article 1, sole paragraph, declares that all political power emanates from the people. If sovereignty belongs to the people, then the mechanisms through which that sovereignty is exercised should remain subject to meaningful public verification.

Taken together, these constitutional provisions support an interpretation that transparency should be maximized whenever possible, particularly regarding the software responsible for recording and counting votes.

3. The Access to Information Act

The Brazilian Access to Information Act establishes publicity as the general rule and confidentiality as the exception(Ivanova & Myltykbaev, 2022).

Whenever information is withheld from public disclosure, the restriction should possess a legal basis, satisfy the statutory requirements for confidentiality, and, where applicable, remain subject to formal classification and temporal limitations(Ivanova & Myltykbaev, 2022).

According to this thesis, indefinite or effectively permanent non-disclosure of election software is difficult to reconcile with this legal framework unless expressly justified within the procedures established by the Access to Information Act.

4. Technical Verifiability

Merely allowing limited institutional inspection of source code does not produce complete public verifiability.

Meaningful independent verification would require public access to:

- the complete source code;

- compiler versions;

- build scripts;

- third-party dependencies;

- operating system configuration;

- environment variables;

- deterministic build procedures;

- cryptographic hashes of official binaries.

Using reproducible builds, independent researchers could compile the software themselves and verify that their binaries are bit-for-bit identical to those officially deployed.

This approach minimizes institutional trust while maximizing objective verification.

5. Transparency and Election Integrity

Transparency and security should not be viewed as opposing principles.

Modern cybersecurity increasingly recognizes that publicly reviewable systems frequently benefit from broader expert scrutiny, allowing vulnerabilities to be identified and corrected before they can be exploited.

For election infrastructure, public verifiability strengthens institutional legitimacy because confidence derives from independently reproducible evidence rather than exclusive governmental access.

6. The Regulatory Issue

Under this thesis, any administrative regulation that permanently prevents public verification of election software exceeds the proper scope of administrative rulemaking if it effectively limits constitutional rights without explicit legislative authorization.

If temporary confidentiality is considered necessary before an election for operational security reasons, such restrictions should remain exceptional, formally justified, and limited in duration.

Once the election has concluded—or after any legally authorized confidentiality period expires—the software and every artifact necessary for deterministic verification should become publicly available.

Conclusion

This thesis concludes that democratic legitimacy is strengthened when election software is independently verifiable by any technically qualified citizen.

Accordingly, regulations that indefinitely prevent the publication of the election source code, deterministic build environment, and verification artifacts are argued to be inconsistent with the constitutional principles of publicity, democratic accountability, and public oversight, as well as with the interpretative framework established by Brazil's Access to Information Act.

Under this constitutional interpretation, the eventual public disclosure of the complete election software ecosystem is not merely a matter of administrative convenience but a democratic requirement.